IN THE CLAIMS

Please amend the claims as follows:

1. (Currently amended) A method comprising:

performing an authentication of a computing device and equipment of an operator of services for the computing device for a session of communication between the computing device and the equipment, the performing comprising:

generating, in the computing device, a random number;

generating a one-time-pad key based on a hash operation of a value selected from the group consisting of an identification of the computing device, an identification of the equipment, a platform configuration measurement of the computing device stored in a protected storage within the computing device and an identification of the session of communication stored in the protected storage within the computing device;

encrypting the random number based on the one-time-pad key;

transmitting the encrypted random number to the equipment;

receiving, from the equipment, an encrypted value in response to the encrypted random number, wherein the encrypted value includes a challenge of a challenge-response;

verifying the encrypted value;

encrypting a response to the challenge of the challenge-response;

transmitting the response to the equipment; and

receiving, from the equipment, an authentication verification; and

auditing the authentication, wherein auditing comprises:

storing at least one attribute of the authentication into an audit log within a memory of the computing device;

encrypting the audit log based on an encryption key that is generated and stored within the computing device;

generating an integrity metric of the audit log; and

generating a signature of the integrity metric with a signature key that is generated and stored within the computing device.

2. (Original) The method of claim 1, wherein the platform configuration measurement of the computing device comprises a version of hardware in the computing device.

3. (Original) The method of claim 1, wherein the platform configuration measurement of the computing device comprises a version of software executing in the computing device.

4. (Original) The method of claim 1, wherein the challenge of the challenge-response comprises an encryption of a data string that includes a concatenation of the random number generated in the computing device, a random number generated by the equipment and the identification of the session.

5. (Original) The method of claim 4, wherein the response of the challenge-response comprises an encryption of a data string that includes a concatenation of the random number generated in the computing device and the random number generated by the equipment.

6. (Canceled)

7. (Currently amended) The method of claim [[6]] 1, wherein auditing the authentication further comprises generating a signature of a value of an audit counter with the signature key.

8. (Currently amended) A method comprising:

authenticating a computing device and a different entity for a session of communication between the computing device and the different entity, the authenticating comprising:

generating a hash of a value selected from the group consisting of a platform configuration value associated with computing device stored in the computing device and the identification of the session stored in a protected storage within the computing device and;

encrypting a random number based on the hash; [[and]]

transmitting the encrypted random number to the different entity; and

auditing the authenticating, wherein auditing comprises,

storing at least one attribute of the authenticating into an audit log within a memory of the computing device;

encrypting the audit log based on an encryption key that is generated and stored within the computing device;

generating an integrity metric of the audit log; and

generating a signature of the integrity metric with a signature key that is generated and stored within the computing device.

9. (Original) The method of claim 8, wherein the authenticating further comprises:
encrypting a response to a challenge of a challenge-response, wherein the challenge is received, in response to the encrypted random number, as part of an encrypted value from the different entity; and

transmitting the encrypted response to the different entity.

10. (Original) The method of claim 8, further comprising commencing a transaction between the computing device and the different entity, after receiving an authentication verification message in response to the encrypted response from the different entity.

11. (Canceled)

12. (Currently amended) The method of claim [[11]] 8, wherein auditing the authenticating further comprises generating a signature of a value of an audit counter with the signature key.

13. (Original) The method of claim 12, wherein auditing the authenticating further comprises appending the integrity metric, the signature of the integrity metric, the signature of the value of the audit counter and the value of the audit counter to the audit log.

14. (Original) The method of claim 8, wherein the platform configuration value associated with the computing device comprises a version of hardware in the computing device.

15. (Original) The method of claim 8, wherein the platform configuration value associated with the computing device comprises a version of software executing in the computing device.

Claims 16-24. (Canceled)

25. (Currently amended) A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

performing an authentication of a computing device and equipment of an operator of services for the computing device for a session of communication between the computing device and the equipment, the performing comprising:

generating, in the computing device, a random number;

generating a one-time-pad key based on a hash operation of a value selected from the group consisting of an identification of the computing device, an identification of the equipment, a platform configuration measurement of the computing device stored in a protected storage within the computing device and an identification of the session of communication stored in the protected storage within the computing device;

encrypting the random number based on the one-time-pad key;

transmitting the encrypted random number to the equipment;

receiving, from the equipment, an encrypted value in response to the encrypted random number, wherein the encrypted value includes a challenge of a challenge-response;

verifying the encrypted value;

encrypting a response to the challenge of the challenge-response;

transmitting the response to the equipment; and

receiving, from the equipment, an authentication verification; and

auditing the authentication, wherein auditing comprises:

storing at least one attribute of the authentication into an audit log within a memory of the computing device;

encrypting the audit log based on an encryption key that is generated and stored within the computing device;

generating an integrity metric of the audit log; and

generating a signature of the integrity metric with a signature key that is generated and stored within the computing device.

26. (Original) The machine-readable medium of claim 25, wherein the challenge of the challenge-response comprises an encryption of a data string that includes a concatenation of the random number generated in the computing device, a random number generated by the equipment and the identification of the session.

27. (Original) The machine-readable medium of claim 26, wherein the response of the challenge-response comprises an encryption of a data string that includes a concatenation of the random number generated in the computing device and the random number generated by the equipment.

28. (Currently amended) A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

authenticating a computing device and a different entity for a session of communication between the computing device and the different entity, the authenticating comprising:

generating a hash of a value selected from the group consisting of a platform configuration value associated with computing device stored in the computing device and the identification of the session stored in a protected storage within the computing device and;

encrypting a random number based on the hash; [[and]]

transmitting the encrypted random number to the different entity; and

auditing the authenticating, wherein auditing comprises,

storing at least one attribute of the authenticating into an audit log within a memory of the computing device;

encrypting the audit log based on an encryption key that is generated and stored within the computing device;

generating an integrity metric of the audit log; and

generating a signature of the integrity metric with a signature key that is generated and stored within the computing device.

29. (Original) The machine-readable medium of claim 28, wherein the authenticating further comprises:

encrypting a response to a challenge of a challenge-response, wherein the challenge is received, in response to the encrypted random number, as part of an encrypted value from the different entity; and

transmitting the encrypted response to the different entity.

30. (Original) The machine-readable medium of claim 28, further comprising commencing a transaction between the computing device and the different entity, after receiving an authentication verification message in response to the encrypted response from the different entity.

Claims 31-33. (Canceled)

34. (New) The machine-readable medium of claim 25, wherein the platform configuration measurement of the computing device comprises a version of hardware in the computing device.

35. (New) The machine-readable medium of claim 25, wherein the platform configuration measurement of the computing device comprises a version of software executing in the computing device.

36. (New) The machine-readable medium of claim 25, wherein auditing the authentication further comprises generating a signature of a value of an audit counter with the signature key.